

NO. 17-15611-BB

**IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT**

**UNITED STATES OF AMERICA,
*Plaintiff/appellee,***

v.

**SCOTT JOSEPH TRADER,
*Defendant/appellant.***

**On Appeal from the United States District Court
for the Southern District of Florida**

**REPLY BRIEF OF THE APPELLANT
SCOTT JOSEPH TRADER**

**MICHAEL CARUSO
Federal Public Defender**

**Fletcher Peacock
Assistant Federal Public Defender
Attorney for Appellant Trader
109 North 2nd Street
Fort Pierce, Florida 34950
Tel. (772) 489-2123**

**THIS CASE IS ENTITLED TO PREFERENCE
(CRIMINAL APPEAL)**

**CERTIFICATE OF INTERESTED PERSONS
AND CORPORATE DISCLOSURE STATEMENT**

**United States v. Scott Joseph Trader
Case No. 17-15611-BB**

Appellant files this Certificate of Interested Persons and Corporate Disclosure Statement, listing the parties and entities interested in this appeal, as required by 11th Cir. R. 26.1.

Barnes, Antonia J., Assistant United States Attorney

Cannon, Aileen M., Assistant United States Attorney

Carlton, Stephan, Assistant United States Attorney

Caruso, Michael, Federal Public Defender

Fajardo Orshan, Ariana, United States Attorney

Ferrer, Wifredo A., Former United States Attorney

Greenberg, Benjamin G., Former United States Attorney

Gyires, Marton, Assistant United States Attorney

Hernandez, Christine, Assistant United States Attorney

Hopkins, Hon. James M., United States Magistrate Judge

Marks, Neison, Assistant Federal Public Defender

Matthewman, Hon. William, United States Magistrate Judge

Maynard, Hon. Shaniek M., United States Magistrate Judge

Middlebrooks, Hon. Donald M., United States District Judge

Militello, Kristy, Assistant Federal Public Defender

Minor Victim 1

Minor Victim 2

Minor Victim 3

Peacock, R. Fletcher, Assistant Federal Public Defender

Rubio, Lisa Tobin, Assistant United States Attorney

Smachetti, Emily M., Assistant United States Attorney

Trader, Scott Joseph, Defendant/Appellant

United States of America, Plaintiff/Appellee

Villafana, Marie, Assistant United States Attorney

s/Fletcher Peacock

Fletcher Peacock

Assistant Federal Public Defender

TABLE OF CONTENTS

CERTIFICATE OF INTERESTED PERSONS	C-1
TABLE OF CITATIONS	iii
REPLY ARGUMENT AND CITATIONS OF AUTHORITY	1
1. Whether the government’s procurement of the defendant’s “Kik” subscriber records, including location information, without a warrant was a violation of Mr. Trader’s reasonable privacy expectation under the Fourth Amendment.....	1
A. The government violated Mr. Trader’s expectation of privacy in his physical movements when it requested 30 days of location information without a warrant.	1
B. As in <i>Carpenter</i> , the instant Kik data is “cell phone location records,” and due to their unique nature they constitute an exception to the third party doctrine.....	8

C.	The defendant’s case is distinguishable, factually and legally, from all pre- <i>Carpenter</i> cases which have dealt with the privacy of IP addresses under the Fourth Amendment.	12
D.	Compliance with The Stored Communications Act is irrelevant to whether the defendant had a reasonable expectation of privacy in the information obtained from Kik.	14
2.	Whether the affidavit in support of the warrant to search Mr. Trader’s home failed to show probable cause on its face.....	15
A.	The search warrant affidavit failed to establish a link between the residence to be searched and the criminal activity perceived.....	15
CONCLUSION		18
CERTIFICATE OF COMPLIANCE.....		19
CERTIFICATE OF SERVICE.....		20

TABLE OF CITATIONS

CASES:

Carpenter v. United States,

____ U.S. ____, 138 S.Ct. 2206 (2018) *passim*

Ferguson v. City Of Charleston,

532 U.S. 67, 121 S.Ct. 1281 (2001) 9

Guest v. Leis,

255 F.3d 325 (6th Cir. 2000) 13

Kyllo v. United States,

533 U.S. 27, 121 S.Ct. 2038 (2001) 6-8

Payton v. New York,

445 U.S. 573, 100 S.Ct. 1371 (1980) 6

Riley v. California,

573 U.S. 373, 134 S.Ct. 2473 (2014) 10

Smith v. Maryland,

442 U.S. 735, 99 S.Ct. 2577 (1979) 9-10, 14

Stoner v. California,

376 U.S. 483, 84 S.Ct. 889 (1964) 9

United States v. Beckett,

369 F. App'x. 52 (11th Cir. 2010)13-14

United States v. Forrester,

512 F.3d 500 (9th Cir. 2008) 13

United States v. Graham,

796 F.3d 332 (4th Cir. 2015) 8

United States v. Hambrick,

225 F.3d 656 (4th Cir. 2000) 14

United States v. Jacobson,

466 U.S. 109, 104 S.Ct. 1652 (1984)9

United States v. Jones,

565 U.S. 400, 132 S.Ct. 945 (2012) 5

United States v. Karo,

468 U.S. 705, 104 S.Ct. 3296 (1984).....6-8

United States v. Miller,

425 U.S. 435, 96 S.Ct. 1619 (1976)9-10

United States v. Weast,

811 F.3d 743 (5th Cir. 2016) 13

STATUTORY AND OTHER AUTHORITY:

U.S. Const. amend. IV	<i>passim</i>
18 U.S.C. § 2702(a)(8).....	4
18 U.S.C. § 2703	14
18 U.S.C. § 2703(d).....	14-15
https://en.wikipedia.org/wiki/Cellular_network	5
https://www.reddit.com/r/KinFoundation/comments/8wvrsq/ stats_917_million_monthly_users_of_Kik_as_of_may/	11

REPLY ARGUMENT AND CITATIONS OF AUTHORITY

Issue I

Whether the government's procurement of the defendant's "Kik" subscriber records, including location information, without a warrant was a violation of Mr. Trader's reasonable privacy expectation under the Fourth Amendment.

A. The government violated Mr. Trader's expectation of privacy in his physical movements when it requested 30 days of location information without a warrant.

By sending an emergency request to Kik, requesting the disclosure of "all recent IP addresses used by the account holder" and all basic subscriber information, law enforcement violated Mr. Trader's Fourth Amendment reasonable expectation of privacy. The warrantless seizure resulted in the disclosure of 30 days of detailed location information. In response to the request, Kik disclosed 26 pages of historical IP addresses, remote ports accessed, the type of connection device, the transactional chat log time stamp, and the corresponding date and time that each message was sent and received. This includes 593 different location points over 30 days, the date and time that the defendant was at each location, the type of device used, and the specific device identifier information for each device.

In *Carpenter*, the Supreme Court held that mapping the past movements of a cell phone over seven days, “provides an all-encompassing record of the holder’s whereabouts. As with GPS information, the time stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his familial, political professional, religious, and sexual associations.” 138 S.Ct. at 2217. Here, law enforcement was essentially given data that was equally as invasive, if not more, than the cell site location information (CSLI) at issue in *Carpenter*. Due directly to the location information given to law enforcement by Kik, the agents were not only able to identify and locate the defendant, but also to look through that “intimate window” to see where the defendant spent most of his time, i.e., at his home.

Because 413 of the revealed location points were from the home IP address, and the connections were through a wireless network (WiFi), law enforcement was able to place the device, and by default the owner of the device, at the physical location of the IP address. And not only did this permit the agents to know where Mr. Trader had been, it also allowed them to view patterns of the defendant’s activity and to predict

where he would be in the future. A mapping of the account activity for the defendant's Kik account reveals that during the overnight hours, every night from May 1st through May 31st of 2017, the defendant and his cell phone were at one location only. This "intimate window into a person's life" revealed where the defendant was on 30 consecutive days and nights.

Coincidentally, the search of the defendant's residence occurred the day after the location records ended, June 1st, and at the same time the location records indicated that he would be present, 1:10 a.m. (DE 14-1, 17). The agents never physically observed the defendant at his residence and they did not need to do so. They already had him under round-the-clock surveillance by means of 30 days of Kik records.

"The retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to [the location information here], the government can now travel back in time to retrace a person's whereabouts . . . Police need not even know in advance whether they want to follow a particular individual, or when . . . whoever the suspect

turns out to be, he has effectively been tailed every moment of every day . . . without regard to the constraints of the Fourth Amendment.” *Carpenter*, 138 S.Ct. at 2218.

Additionally, law enforcement was able to learn the habits and patterns of the defendant through his Kik account data. At the very least, by mapping his locations, law enforcement was able to deduce the daily routine of the defendant from one day to the next. For example, without identifying any other locations than the defendant’s home, law enforcement could conclude when he was at home, when he left and returned home, the amount of time he was gone, and his sleep and wake habits. This information is available simply from the Kik account data.

The data released by Kik also showed the defendant connecting at IP addresses other than his home.¹ Through the same means used to learn the location of his home IP address, i.e. a § 2702(a)(8) request, law enforcement was able to determine the location of the other IP addresses and track the defendant’s movements among those locations over the 30 day period. Such information is not significantly distinguishable from the CSLI addressed in *Carpenter*.

¹ Kik is a mobile application which operates exclusively with cellular phones. Consequently, it documents use of the application from whatever mobile or static IP address used by the cellular phone.

There was additional information about the defendant gathered through the Kik records. A total of 593 contacts from 42 different IP addresses were recorded. Of those 593 contacts, 413 of them show the defendant at his home IP address. However, 180 contacts were made from other IP addresses over Mobile LTE or Mobile Hot Spot networks.² Therefore, in addition to 413 contacts from the defendant's home, law enforcement was given the means to follow 180 separate contacts among numerous other mobile network locations. This can't be viewed as anything other than "tracking" a person's movements and locations. As they would with any subject, these tracked waypoints would show the defendant's work route as a pool technician, trips to the county courthouse, and trips with his family, all of which were made on public roads by automobile.

The tracking of a person's movements in this case is the same wrong addressed in *Carpenter*. The only difference is the means used by law enforcement to do the tracking. Both means have many of the qualities of the GPS monitoring considered in *United States v. Jones*, 565 U.S. 400, 132 S.Ct. 945 (2012). There, the court found that the

² Contacts made through Mobile LTE are made through the same "cell towers" used to compile the data in *Carpenter*. See generally, https://en.wikipedia.org/wiki/Cellular_network

attachment of a GPS device to an automobile was a search under the Fourth Amendment. “[The GPS device] is detailed, encyclopedic, and effortlessly compiled.” And so is the information here. It is automatically and effortlessly recorded. There is no conscious relinquishment by the subject. It is detailed to the extent of every mobile or static access of the application. And since Kik is a password protected application, it permits law enforcement to verify the identity of the user with greater certainty than CSLI. Like Carpenter and Jones, the defendant had a reasonable expectation of privacy in the movements recorded. Again, there is no meaningful distinction.

And it cannot be questioned that citizens have a heightened expectation of privacy in their own homes. *See generally, United States v. Karo*, 468 U.S. 705, 104 S.Ct. 3296 (1984) (government not free to monitor beepers in private residence without a warrant). “We have said that the Fourth Amendment draws ‘a firm line at the entrance to the house’ . . . That line, we think, must not only be firm but also bright.” *Kyllo v. United States*, 533 U.S. 27, 40, 121 S.Ct. 2038, 2046 (2001) (quoting *Payton v. New York*, 445 U.S. 573, 100 S.Ct. 1371 (1980)).

In the instant case, 413 of the recorded contacts and locations were in the defendant's home. As previously noted, law enforcement was also made privy to the times of contact over the entire 30 day period. This information is arguably greater than that considered in *Kyllo* and *Karo*. In *Kyllo*, law enforcement simply conducted thermal imaging of a home for "a few minutes." In *Karo*, law enforcement delivered a container with a concealed beeper to a home and monitored the beeper while it was in the home. In both cases, the Supreme Court found that a warrant was required. In both cases, the Court essentially held that officers can't simply do through technology what could not do in person. Here, the principles should apply in the same fashion. Homeland Security agents could not have entered the defendant's home to determine whether he was there on 413 occasions without a warrant. Under *Kyllo* and *Karo*, they should not be able to do the same thing through an emergency request. A warrant was required.

Further, *any* unreasonable intrusion into the sanctity of the home is sufficient to require a warrant. "The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of the information obtained . . . In the home, our cases show,

all details are intimate details, because the entire area is held safe from prying government eyes.” *Kyllo*, 533 U.S. at 37, 121 S.Ct. at 2045 (emphasis in original). “The *Karo* and *Kyllo* courts recognized the location of a person and her property within a home at a particular time as a ‘critical’ private detail protected from the government’s intrusive use of technology.” *United States v. Graham*, 796 F.3d 332, 346 (4th Cir. 2015).

Here, law enforcement used Kik’s historical IP address contacts to locate and surveil the defendant in his home hundreds of times over a 30 day period. Prior to demanding the information, law enforcement did not know the defendant’s identity or location. Law enforcement used technology not generally used by the public to essentially reach through the defendant’s cellular phone application and into his home. In doing so, they violated his right to a reasonable expectation of privacy in his own home.

B. As in *Carpenter*, the instant Kik data is “cell phone location records,” and due to their unique nature they constitute an exception to the third party doctrine.

While it remains the law that an individual generally loses her expectation of privacy in information turned over to a third party,

Smith v. Maryland, 442 U.S. 735, 99 S.Ct. 2577 (1979), information in the hands of a third party is not categorically excluded from protection under the Fourth Amendment. *See, Carpenter v. United States*, ___ U.S. ___, 138 S.Ct. 2206 (2018); *Ferguson v. City Of Charleston*, 532 U.S. 67, 121 S.Ct. 1281 (2001) (patient retained an expectation of privacy in drug tests done without patient’s permission); *United States v. Jacobson*, 466 U.S. 109, 104 S.Ct. 1652 (1984) (sealed letters and packages in the hands of a commercial carrier are still effects in which the sender has an expectation of privacy); *Stoner v. California*, 376 U.S. 483, 84 S.Ct. 889 (1964) (hotel room renter retains expectation of privacy in room’s contents despite hotelier’s consent to search).

Smith and *United States v. Miller* 425 U.S. 435, 96 S.Ct. 1619 (1976) are distinguishable from the facts of this case for multiple reasons. “There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.” *Carpenter*, 138 S.Ct. at 2219.

First, *Smith* and *Miller* did not concern a record of the physical movements of the defendant. *Smith* involved a pen register, which

revealed “little or no identifying information.” *Smith*, 442 U.S. at 742, 99 S.Ct. at 2577. *Miller* involved checks, which the issuer loses control of when the check is negotiated. The instant records contain a comprehensive timeline of the defendant’s location over a month-long period. They are significantly more detailed and intrusive than a pen register or a cancelled check. And notwithstanding that the records were generated for a commercial purpose, a citizen maintains an “anticipation of privacy in his physical location.” *Carpenter*, 138 S.Ct. at 2217.

Second, the instant case involved the tracking of a cellular phone, as in *Carpenter*. Kik is exclusively a cellular phone application. The *Carpenter* Court was not concerned by the *means* of tracking a cellular phone; it was concern about the *effect* of tracking that caused the Court to carve an exception from *Smith* and *Miller*. The Court noted that the cellular phone has become “almost a feature of the human anatomy,” its tracking “achieves near perfect surveillance, as if it had attached an ankle monitor to the phone’s user.” 138 S.Ct. at 2218; *see also*, *Riley v. California*, 573 U.S. 373, 393, 134 S.Ct. 2473, 2489 (2014) (discussing the unique nature of modern cellular phones in the context of Fourth

Amendment privacy concerns). In the instant case, the defendant was accessing Kik an average of 20 times per day over the 30 day period. Each access recorded his location, and thus his movements. “Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user’s claim to Fourth Amendment protection.” *Carpenter*, 138 S.Ct. at 2217. The instant Kik records are unquestionably “cell phone location records.”

Finally, as in *Carpenter*, the information obtained was totally retrospective in nature. It was obtained with little or no effort and expense. Kik, presumably collects the same records on all of its customers.³ “[T]he government can now travel back in time to retrace a person’s whereabouts, subject only to the retention policies of the wireless carriers . . . this newfound tracking capacity runs against everyone.” 138 S.Ct. at 2218. Law enforcement can effortlessly, and without expense, obtain the intimate day-to-day past movements of any

³ As of May of 2018, Kik was reported to have over 9,000,000 monthly users. See, https://www.reddit.com/r/KinFoundation/comments/8wvrsq/stats_917_million_monthly_users_of_Kik_as_of_may/

particular person using the application.⁴ For this degree of intrusion a warrant must be required.

Therefore, based upon the factors relied upon in *Carpenter*, the instant case presents the same concerns and an equal, or even greater, invasion into the privacy of a citizen's location. Suppression in this case does not call for an extension of *Carpenter*; it is simply the proper application of the holding in *Carpenter*.

C. The defendant's case is distinguishable, factually and legally, from pre-*Carpenter* cases which have dealt with the privacy of IP addresses and subscriber information under the Fourth Amendment.

The government relies heavily on pre-*Carpenter* case law for the proposition that an individual's IP address and other subscriber information are not protected under the "third party doctrine." Gov. Brief, at 18 – 21. While this point may be accurate, it misses the issue in this case. The essence of the defendant's position is not that his IP address and/or subscriber information are *per se* protected. Rather, it is that law enforcement obtained much more than just that information. It received Kik cellular phone account activity information, from which

⁴ Kik accounts are password protected, thus indicating the identity of the user as well as the location.

it could, and did, deduce the defendant's location, movements, timing and patterns of activity. Law enforcement then used that information to obtain a search warrant and to bolster its evidence of guilt. This was much more than just obtaining an IP address and some subscriber information.

The pre-*Carpenter* cases cited by the government do not deal with the tracking of IP addresses used by a cellular phone. Instead they addressed the privacy of an IP address and subscriber information in the context of desk top or laptop computers connected to a static IP address. There is no tracking capability or concern in those cases. No one carries their desk top computer from location to location, accessing Internet in a mobile capacity. Nor has the laptop computer become "almost a feature of human anatomy." Conversely, a cellular phone (the only means of accessing Kik) does automatically access cellular towers and/or Internet "hot spots" every time it is transported. An IP address is simply another means that can be used to track the cellular phone.

The government relies upon *United States v. Beckett*, 369 F. App'x. 52 (11th Cir. 2010); *United States v. Weast*, 811 F.3d 743 (5th Cir. 2016); *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008); *Guest v.*

Leis, 255 F.3d 325 (6th Cir. 2000); and *United States v. Hambrick*, 225 F.3d 656 (4th Cir. 2000). All of these cases pre-date *Carpenter*. All appear to have dealt with desk top or laptop computers connected to a fixed location and static IP address. None of the cases dealt with cellular phones and none dealt with obtaining mobile location data and movement.

In *Beckett*, a panel of this Court relied upon the proposition that: “The Supreme Court ‘consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.’” 369 F.App’x. at 56 (quoting *Smith v. Maryland*). The defendant respectfully suggests *Carpenter* has drastically changed that proposition and that *Becketts*’ premise has been abrogated when the information obtained permits law enforcement to track a subject’s movements and location through her cellular phone.

D. Compliance with The Stored Communications Act is irrelevant to whether the defendant had a reasonable expectation of privacy in the information obtained from Kik.

In *Carpenter*, it was uncontested that law enforcement had complied with 18 U.S.C. § 2703(d), a companion provision of the Stored Communications Act, and received a court order for production.

Notwithstanding that compliance, the Court found that the required proof for an order, “falls well short of the probable cause required for a warrant . . . an order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records. Before compelling a wireless carrier to turn over a subscriber’s CSLI, the Government’s obligation is a familiar one – get a warrant.” 138 S.Ct. at 2221. As in *Carpenter*, the government’s claim of statutory compliance is irrelevant.

Issue II

Whether the affidavit in support of the warrant to search Mr. Trader’s home failed to show probable cause on its face.

A. The search warrant affidavit failed to establish a link between the residence to be searched and the criminal activity perceived.

The search warrant affidavit failed to demonstrate a link between the defendant’s mother’s residence and the criminal activity (i.e. distribution of child pornography) seen on the cellular phone application Say Hi. While the affidavit may have stated a connection between the suspected cellular application Say Hi and the application Kik, the Kik application was not in any way involved in the criminal activity. The

affidavit simply explained that the two application accounts were each used by a person named Scott, that the Say Hi user profile referred to a Kik account with user name “Daddyhasafunnyface,” and that the user pictures in the user profiles appeared to be similar to each other and to a photo sent during the illegal Say Hi conversations.

While the affidavit may have sufficiently established that the Say Hi and Kik accounts had the same user, the affidavit did not establish that the same device was used on both accounts or that Kik was used in *any* criminal activity. There is no support for the contention that a search of the physical location of the majority of Kik contacts would lead to evidence of the crime committed on Say Hi.

The affidavit noted that Kik provided “a login history, indicating there were logins to the account from IP address 76.110.46.234 starting 1 May 2017 through 31 May 2017, at 6:36 UTC.” However, the affidavit failed to allege any location for the Kik account logins between 6:56 p.m. and 10:48 p.m. on May 30th when the offense of distribution of child pornography was allegedly committed. In fact, the affidavit made no mention of the IP address location of any Kik login on May 30th. The district court was clearly wrong when it concluded that the

affidavit “provided that the IP address 76.110.46.234 is the one from which defendant logged onto his “Kik” account on the same date that he had the explicit conversation with the minor on Say Hi.” DE 15:11. There was no such information in the affidavit.

As noted earlier, the Kik account was accessed almost 600 times from over 40 different locations during May. It was not static, but was frequently changing location. The affidavit contained no information on the locations of the Say Hi login(s). There was simply no evidence showing that the Say Hi device would be found at the same location logged into by the Kik device. Consequently, the conclusion that it would be found in the same location was nothing more than a hunch. It was not based upon probable cause.

Additionally, the affidavit did not connect the defendant to the residence to be searched. The defendant was never seen at the residence. No vehicle registered to him was seen at the residence. No witnesses associated the defendant with the residence. None of the residence utilities were in his name. The defendant’s driver’s license listed a different address. The only connections alleged were that it was his mother’s residence, the defendant had briefly lived at the residence

before, and that he had received some mail there. These minor facts are not sufficient to support the assumption that the defendant resided there and that evidence of child pornography would be found there.

CONCLUSION

In conclusion, the defendant requests that the Court reverse his conviction and remand with instructions that he be permitted to withdraw his guilty plea, or in the alternative, that his sentence be vacated and the case remanded to the district court for resentencing.

MICHAEL CARUSO
FEDERAL PUBLIC DEFENDER

s/Fletcher Peacock
Fletcher Peacock
Assistant Federal Public Defender
109 North 2nd Street
Fort Pierce, Florida 34950
Telephone No. (772) 489-2123
Email: fletcher_peacock@fd.org

CERTIFICATE OF COMPLIANCE

I CERTIFY that this brief complies with the type-volume limitation and typeface requirements of Fed. R. App. P. 32(a)(7)(B), because it contains 3,587 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

This brief also complies with the requirements of Fed. R. App. P. 32(a)(5) and (a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14 point, Century Schoolbook font.

s/Fletcher Peacock
Fletcher Peacock

CERTIFICATE OF SERVICE

I I HEREBY certify that on this 4th day of March, 2019, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF and sent seven copies to the Clerk of the Court via third party commercial carrier for delivery within three days. I also certify that the foregoing document is being served this day via CM/ECF on Christine Hernandez, Assistant United States Attorney, 99 N.E. 4th Street, Miami, Florida 33132.

s/Fletcher Peacock
Fletcher Peacock